Below are several timely HIPAA e-news items and related articles.

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Have a great day!!!
Ken

Main topics included below and attached are:

SANS Computer Security Bootcamp, Feb. 9 - 14, Monterey, CA
see www.sans.org/Bootcamp.htm
Transactions Compliance Extension - various details
HIPAANOTE - - risk assessment, security regs and risk analysis/risk management
[hipaalive] TCS: HCPCs Code on Outpatient Claims
[hipaalive] RE: SECURITY: ROLE BASED ACCESS CONTROL
[hipaalive] RE: PRIVACY Individually Indentifiable Health Information
[hipaalive] Re: GENERAL: Adjustment Reason Codes
HIPAA Implementation Newsletter - Issue #25 - January 11, 2002 (ATTACHED)

********** Transactions Compliance Extension - various details **********

>>> Stanley Nachimson <SNachimson@CMS.HHS.GOV> 01/09/02 02:31PM >>>

On December 27, 2001, President Bush signed into law H.R. 3323, the Administrative Simplification Compliance Act (now known as Public Law 107-105). This law provides for a one year extension of the date for complying with the HIPAA standard transactions and code set requirements (to Oct 16, 2003) for any covered entity that submits to the Secretary of Health and Human Servcices a plan of how the entity will come into compliance with the requirements by October 16, 2003.

The plan must be submitted by October 15, 2002 and shall be a summary of

(A) An analysis reflecting the extent to which, and the reasons why, the person is not in compliance.

(B) A budget, schedule, work plan, and implementation strategy for achieving compliance.

(C) Whether the person plans to use or might use a contractor or other vendor to assist the person in achieving compliance.

(D) A timeframe for testing that begins not later than April 16, 2003.

The law also requires the Department to develop and promulgate a model compliance form for the plan by March 31, 2002, and to allow for compliance plans to be submitted electronically.

Please note that this legislation kept in place the compliance deadlines for the Privacy Rule (April 14, 2003 for all covered entities except small health plans; April 14, 2004 for small health plans).

The Department will be providing the details of the model form and submission procedures at a later date.

The law also requires that, by Oct 16, 2003, providers stop submitting paper claims and submit claims electronically to Medicare. There are waivers for certain small providers or if there is no method for electronic submission of claims available. CMS will provide further details about these requirements through the regulatory process.

You can read the enrolled version of the bill (the version passed by Congress) at:
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3323.ENR:

The Public Law version is expected to be available at the Government Printing Office shortly.

Stanley Nachimson
Office of Information Services, CMS
410-786-6153

** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
The Legislative History, as provided by AFEHCT, is available for review on our host's site (www.hipaadvisory.com/news).

*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
Below is the "legislative history" that accompanies H.R. 3323. It clarifies the legislative intent behind the legislation.
Points worth noting:
*** Secretary not required to approve compliance plans
*** Secretary is required to widely disseminate reports containing effective solutions to compliance problems.
*** Entities that must send non-compliant transactions because trading partners are not in compliance are not to be penalized by HHS
*** Entities can file a compliance plan any time before Oct. 16, 2002 using

HHS model plan or their own format.
*** Model plan to be concise, a "minimal reporting requirement".
*** Compliance plans provided to NCVHS for analysis will be redacted.
*** the role of the vendor community is recognized. Secretary and NCVHS urged to consult with the vendor community or their representatives directly.

If you wish to discuss this legislative history with me please call 202 244 6450.
Tom Gilligan
Association For Electronic Health Care Transactions(AFEHCT)

*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
You can get a PDF version at http://www.ncpdp.org/hipaa_clarification.pdf

*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***

Since President Bush signed the Administrative Simplification Compliance Act into law, Bill Braithwaite, Jeff Fusile and I have collaborated to prepare a comment document that we think may be helpful. I have included an excerpt of the brief Overview section in this email. If anyone desires the complete 3 page PDF version of our comments, please send an email directly to me **** NOT HIPAALIVE**** - with "ASCA Comments" in the subject
line and I'll email you the complete versionl.

Overview and Commentary on the Impact of the
Administrative Simplification Compliance Act
(Also known as H.R. 3323)

William R. Braithwaite, MD, PhD
Thomas L. Hanks
Jeffrey P. Fusile

Overview

On December 27, 2001, President Bush signed into Law the Administrative Simplification Compliance Act (Compliance Act), also known as H.R. 3323. Now that the President has signed this legislation into law, we thought it would be appropriate to comment and help clarify its meaning and application. Up front, we want to point out that it is misleading to characterize this legislation as a "one year delay" of HIPAA, as many headlines have declared. What the Compliance Act does provide is a mechanism for covered entities to apply for an extension of the compliance date to October 16, 2002, for only the Transaction and Code Sets rule.

This extension is automatic if the covered entity meets certain conditions. The primary condition is the submission of a compliance plan by October 2002. This plan, among other things, requires entities to be ready to test transactions by April of 2003. For most covered entities, this will effectively mean that they have only an additional 6 months to be ready to begin sending and receiving electronic transactions. In addition, there is no delay or extension of the HIPAA privacy compliance date of April 14, 2003.

While there will be no federal penalties for non-compliance during this 6-month testing period (April 2003 to October 2003), there will be considerable exposure to business risk and relationship concerns for those who are not capable of performing at an industry acceptable level. Further, many covered entities are looking to early compliance to maintain momentum and establish competitive advantages. This is especially true of the providers, who have the most to gain from the transaction efficiencies and who were least excited about the extension of the compliance date. Many payers will also look to early compliance to maintain momentum and more importantly to improve their relations with their respective provider community(s). In addition, Clearinghouses and key business associates may experience the most dramatic impact as this testing period will be essential to gain the trust and confidence of their payer and provider clientele.

Having been very close to this legislation, we feel it is important to state that there appears to be little, if any chance that this date will be further extended. October 16, 2003 is a date that should be viewed as a definitive "line in the sand". We make this observation for two reasons. First, both the U.S. Senate and the House of Representatives have made it very clear that this extension was provided with great hesitation and the conditions applied to the extension should be viewed as a clear message that another extension is unlikely. Second, if a covered entity cannot submit standard claims to Medicare by October 16, 2003, then Medicare intermediaries and carriers will not accept the claims. In fact, with some exceptions for only the very smallest providers, this legislation prohibits Medicare from accepting paper claims at all after October 16, 2003. This is an attention getting provision for covered entities conducting Medicare transactions. In fact, it is likely that many other government and commercial payers will use this precedent to adopt similar policies.

I hope this helps,

Thanks,

Tom Hanks
Director Client Services
Health Care Practice

PricewaterhouseCoopers, LLP
Chicago, IL
Ph: 312.298.4228
Email: Tom.Hanks@us.pwcglobal.com

********** HIPAANOTE
****
==========
==========
H I P A A N O T E -- Volume 2, Number 2 -- January 11, 2002
>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <
==========
==========
** "Between a Rock and a Hard Place: Assessing the Impacts of the TCS Compliance Extension" Audio Conference **

Join us for this intensive 60-minute audio discussion plus presentation slides by Phoenix Health Systems' Principal Clyde Hewitt on Thursday, January 24, 2002, at 2:00 PM EST

SIGN UP NOW! Go to:
http://www.hipaadvisory.com/ezcart/index.cfm?0111n
==========
==========

This week's HIPAAnote...

*** HIPAA Terms: Risk Assessment, Risk Analysis, Risk Management ***

There is a lot of confusion between the terms Risk Assessment, Risk Analysis and Risk Management with regards to what is required by the HIPAA proposed security standards. Let's discuss your Security Management Program and how these basic components will help ensure that it is cost effective, documented and allocates security resources appropriately.

Risk is the possibility of something adverse happening. Risk assessment is not defined by HIPAA; however, it is commonly accepted as the process of defining deficiencies or "gaps" in your current security program. We prefer the term GAP analysis or Impact Analysis. This analysis is the first component of becoming HIPAA compliant.

Security Management includes both Risk Analysis and Risk Management. This risk-based Security Management process allows you the ability to ensure that your HIPAA security solutions reflect a balance between risk and cost.

This balance will enable you to ensure that risks are minimized in the most cost effective manner possible.

* Risk Analysis is a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.

* Risk Management is the process of assessing risk, taking steps to reduce the risk to an acceptable level and maintaining that level of risk.

After performing an Impact Analysis of systems and networks, a documented process to determine the best method for remediation must be completed. This is where Risk Analysis and Risk Management come into the picture. To perform Risk Analysis/Risk Management, first determine the risk to the organization and to the Patient Data. List the possible remediation steps, timeframes and resources required (people, money, etc.) Then determine what are the best steps to take to reduce risk to an acceptable level. HIPAA does not require security and risk reduction at any cost; it DOES require documented risk-based decisions.

Here's an example: Let's assume that you determine that your current Disaster Recovery Plan is not adequate. The impact of a loss of data processing capabilities creates an unacceptable risk. The threats of fire, tornado, or floods are real threats. The probability of the risk (threats) is low, but the impact is high. You research your best options and find that you can:

1) utilize a vendor to provide a hot-site location for $10,000 per month, OR
2) build a redundant data center at a cost of $2,500,000.

You can then make a documented decision to utilize the hot-site as a reasonable cost effective step to reduce the risk to an acceptable level.

Here's another example: A primary clinical system in use does not provide audit trail. You determine that this creates an unacceptable risk (Threat) to patient data, as unauthorized users can view patient records without detection. The probability of this occurring is high and the impact is also high. Action is required. You determine your options are to:

1) await a vendor release at a cost of $100,000, OR
2) replace the system with a HIPAA security compliant version for $3.5 million.

Now you must make a documented, defendable decision as to which option is in your organization's best interest. The decision may be complicated by additional factors, e.g., resources in the first year for one of the options will

not include audit trail due to vendor resources being focused first on other greater risk-reduction areas.

Risk analysis/risk management allows the institution to review its options to mitigate the risk and choose the best fit for the organization. Document all decisions which will assist in showing due diligence with regards to minimizing risk to acceptable levels. Use these techniques to create a prioritized action plan with acceptable timeframes. Execute this plan and ensure that resources are expended in the most cost-effective method while reducing risk to acceptable levels.

For more information on risk assessment, go to:
http://www.hipaadvisory.com/action/HIPAAssessment.htm?0111n

For more about the security regs and risk analysis/risk management, go to:
http://www.hipaadvisory.com/regs/securityandelectronicsign/index.htm

That's today's HIPAAnote...now, pass it along!

==========
HIPAAnotes are published weekly as a learning tool to help you and your associates stay tuned-in to HIPAA and its implications. Forward it to anyone with a "need to know" through your own internal mailing list, intranet or newsletter -- whatever works for you....

Our HIPAAcratic oath: We'll use your ideas for HIPAAnotes -- send them!
E-mail D'Arcy Gue, Editor: info@phoenixhealth.com
==========

********** [hipaalive] TCS: HCPCs Code on Outpatient Claims **********
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
http://www.hipaa-dsmo.org/faq/X12N.asp
I have used this site for questions on X12 transactions. They should be able to help you.
Peggy Drake

********** [hipaalive] RE: SECURITY: ROLE BASED ACCESS CONTROL **********
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
If you haven't already, check out
http://www.sans.org/infosecFAQ/securitybasics/RBAC.htm
<http://www.sans.org/infosecFAQ/securitybasics/RBAC.htm> which has a great
primer on role-based access.
Regards,

Kevin Johnston, RN
Coordinator for Security & Privacy
PeaceHealth Oregon Region

***** [hipaalive] RE: PRIVACY Individually Indentifiable Health Information *********
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
The University as a whole is a hybrid entity. It is an organization that has, as its primary purpose, the accomplishment of functions that are not HIPAA-related. At the same time, certain departments of the University perform certain covered functions. The specific departments that use and disclose PHI to carry out these covered functions must meet the applicable HIPAA privacy regulation requirements, but the other departments are not required to do so. The University must establish a "privacy wall" between the departments to ensure that PHI is not communicated to people outside the
health care component of the organization. The details of these safeguard requirements are spelled out in the privacy regulation at ? 164.504.

Bye for now -- Harry

Harry E. Smith, CISSP
Principal and Founder
Timberline Technologies LLC
10300 West 23rd Avenue
Lakewood, CO 80215
303-717-0793

-----Original Message-----
From: Laura Knoblauch [mailto:Lmknobl@wpgate.shs.ilstu.edu]
Sent: Friday, January 04, 2002 11:03 AM
To: HIPAAlive Discussion List
Subject: [hipaalive] PRIVACY Individually Indentifiable Health Information

*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***

On page 82493 under Individually Identifiable Health Information, the section refers to employers in addition to health care providers, health plans and health care clearinghouses. However, employers are not included in the covered entity definition on page 82476.

My questions:

1. A University, which has departments who employ health care providers such as Student Health Service, Counseling Center, Speech and Hearing Clinic are covered entities; are the individual departments covered entities or is the University as a whole the covered entity?

2. Will the University Human Resource Dept, Disability Concerns, Safety Office and other various offices on campus also be required to meet the Privacy Regulations because they receive Individually Identifiable Health Information as an employer from a covered entity even though they did not create it as a health care providers, health plans and health care clearinghouses?

Any feedback is appreciated.

Laura

********** [hipaalive] Re: GENERAL: Adjustment Reason Codes **********
*** HIPAAlive! From Phoenix Health Systems/HIPAAdvisory.com ***
The Health Care Code Maintenance Committee (HCCMC) that maintains the Claim Adjustment Reason Codes and the Claim Status Codes usually meets from 1:00 - 4:00 PM the Sunday before each X12 Trimester Meeting. Thus, the next meeting should be on Sunday, February 3, in Seattle. You can make code maintenance requests online at http://www.wpc-edi.com/CommitteeC_40.asp.

You need to be aware that getting new reason codes approved is very challenging, and for good reason. Payers frequently have thousands of distinct payment codes. But the reason codes are supposed to be limited to unique ways that a payment can be automatically posted. Far fewer distinctions are needed for this purpose than for explaining how a health plan's benefits work. And, as nearly as possible, they need to be unambiguous with respect to all pre-existing reason codes, so that a newcomer has half a chance of guessing correctly regarding what code to use for a given purpose.

I don't mean to discourage you here. It's just that you really need to do your homework first, and I would guess that the vast majority of such requests are resolved by identifying which of the existing reason codes can be used for the identified purpose, rather than by adding new codes. There are less than 200 such codes at present.

The point of all of this is to keep the 835 transaction as simple as possible from a provider's perspective.

Good luck!

- Zon Owen -
(808)597-8493

----- Original Message -----
From: "Jones, Nancy" <njones@bcbsok.com>
To: "HIPAAlive Discussion List" <hipaalive@lists.hipaalert.com>
Sent: Wednesday, January 09, 2002 4:51 AM
Subject: [hipaalive] Re: GENERAL: Adjustment Reason Codes

Our Plan recently completed the mapping of the HIPAA Adjustment Reason Codes. We found a few where there is no match to what we currently use. It
is my understanding that new codes can be requested on-line through CMS. Has anyone had any experiences with requesting new Adjustment Reason Codes
for HIPAA? Do we know what the turn-around time is for requesting these? Are there steps that need to be followed in making a request? Do you have any suggestions on creating the generic Adjustment Reason Code?

Your input is appreciated!
Thank you,
Nancy K. Jones
HIPAA Project Leader, Benefits Administration
Blue Cross Blue Shield of Oklahoma
PO Box 3283
Tulsa, OK 74102-3283

****
****